



Chief Information Officer

Advisory

November 3, 2006

To: Distribution

Subject: Business-Oriented Spam

The State has recently experienced an upsurge in SPAM. (SPAM is defined as unwanted communications received in the form of an email.) Examples of SPAM include adult oriented content or solicitations, pharmaceutical, or fraudulent investment opportunities or other communications. SPAM represents both a significant privacy risk and a security risk, as it can be a vector for potential identity theft, source of additional SPAM, and the introduction of malware into the State's network.

The Office of Cyber Protection is aware of recent increases of SPAM and is actively working with agency email Administrators to improve the State's anti-SPAM capabilities. The State's anti-SPAM security tools continue to be updated with the latest detection software in an effort to reduce the amount of spam experienced by email users. This is an ongoing process as SPAMers continue to refine their techniques.

But as with all computer security issues, the user also has a role in maintaining security; here is what you can do:

SPAM comes in all manner of guises; but regardless of the form, format or content, the guidelines to users for dealing with spam are:

1. Maintain a healthy suspicion of unsolicited or unexpected messages, even from people you know. Any email that is sent to you with your address as the sender can always be considered SPAM.

2. Always treat messages as being potentially fraudulent, because a number of attacks utilize what appear to be legitimate emails from businesses, banks, or other reputable sources.
3. Users must never click on any links contained within suspected SPAM messages. Never click on any of the unsubscribe links, and never reply to SPAM messages.
4. Users should always consider where they distribute their email addresses and to whom they provide this information.
5. Never purchase items from offers that you received through SPAM or other suspicious emails.
6. Never provide any personal information in response to SPAM or other suspicious emails.
7. Users are encouraged to report incidents of spam by forwarding suspected or real spam messages to spamreports@mt.gov
8. If the email looks too good to be true, it more than likely is.

If you have questions or comments, please feel free to contact Dick Clark at (406) 444-2700 or dclark@mt.gov.

To subscribe to automatic Enterprise IT publications notification, please visit:

<http://itsd.mt.gov/policy/itpubnotify.asp>

To subscribe to automatic CIO Advisory notification, please visit:

<http://test.itsd.mt.gov/policy/advisories/cionotify.asp>

Advisory Disposition: Retain 90 days

CIO_ADVRY_20061103